

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Atsuhisa SAITOH, et al.

GAU: 2131

SERIAL NO: 10/665,484

EXAMINER:

FILED: September 22, 2003

FOR: IMAGE FORMING DEVICE CONTROLLING OPERATION ACCORDING TO DOCUMENT
SECURITY POLICY

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

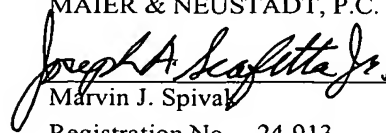
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2002-273985	September 19, 2002
JAPAN	2002-275973	September 20, 2002
JAPAN	2002-297888	October 10, 2002
JAPAN	2002-341222	November 25, 2002
JAPAN	2003-314463	September 5, 2003
JAPAN	2003-314464	September 5, 2003
JAPAN	2003-314465	September 5, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 9 月 1 9 日
Date of Application:

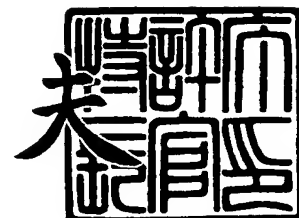
出 願 番 号 特 願 2 0 0 2 - 2 7 3 9 8 5
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 7 3 9 8 5]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0201604

【提出日】 平成14年 9月19日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 15/00

【発明の名称】 複写方法、プログラム、記録媒体、伝送装置及び複写装置

【請求項の数】 15

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 斉藤 敦久

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 金井 洋一

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 谷内田 益義

【特許出願人】

 【識別番号】 000006747

 【氏名又は名称】 株式会社リコー

【代理人】

 【識別番号】 100070150

 【弁理士】

 【氏名又は名称】 伊東 忠彦

【手数料の表示】

 【予納台帳番号】 002989

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 複写方法、プログラム、記録媒体、伝送装置及び複写装置

【特許請求の範囲】

【請求項 1】 複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とする複写方法。

【請求項 2】 更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手順を有し、

上記判断手順は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手順により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断することを特徴とする請求項 1 記載の複写方法。

【請求項 3】 上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むことを特徴とする請求項 1 又は 2 記載の複写方法。

【請求項 4】 上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むことを特徴とする請求項 1 乃至 3 いずれか一項記載の複写方法。

【請求項 5】 上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むことを特徴とする請求項 1 乃至 4 いずれか一項記載の複写方法。

【請求項 6】 上記セキュリティポリシーは、上記ユーザーにより複写が指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの時

刻とを履歴情報として格納する要件を含むことを特徴とする請求項1乃至5いずれか一項記載の複写方法。

【請求項7】 複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法における処理をコンピューターに実行させるためのプログラムであって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とするプログラム。

【請求項8】 複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法におけるコンピューターに実行させるためのプログラムを格納した記録媒体であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とする記録媒体。

【請求項9】 複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行うプログラムをネットワークを介して伝送する伝送装置であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が

複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを他の情報システムに伝送する伝送手順とを有することを特徴とする伝送装置。

【請求項 10】 複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写装置であって、

複写する情報を読み取る読取手段と、

上記読取手段により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手段と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手段と、

上記判断手段の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手段とを有することを特徴とする複写装置。

【請求項 11】 更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手段を有し、

上記判断手段は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手段により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断することを特徴とする請求項 10 記載の複写装置。

【請求項 12】 上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むことを特徴とする請求項 10 又は 11 記載の複写装置。

【請求項 13】 上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むことを特徴とする請求項 10 乃至 12 いずれか一項記載の複写装置。

【請求項 14】 上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むことを特徴とする請求項 10 乃至 13 いずれか一項記載の複写装置。

【請求項 15】 上記セキュリティポリシーは、上記ユーザーにより複写が

指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの時刻とを履歴情報として格納する要件を含むことを特徴とする請求項10乃至14いずれか一項記載の複写装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複写方法に係り、特に、文書に関するセキュリティポリシーに基づいて複写処理を制御する複写方法に関する。

【0002】

また、本発明は、そのような複写方法におけるプログラム、及びそのプログラムを格納した記録媒体、ネットワークを介してそのプログラムを伝送するための伝送装置及びその複写方法における処理を行う複写装置に関する。

【0003】

【従来の技術】

近年、多くのオフィス業務では、ファックス、プリンター、複写機などの情報システムを用いて文書が扱われている。このような情報システムに依存して日常の業務が行われるにつれて、その文書を扱う情報システムのセキュリティ確保が重要視されるようになってきている。特に、最近では官公庁を中心としてISO17799として知られる情報セキュリティ管理標準に基づいて組織の情報セキュリティポリシーを掲げるところが増え、そのポリシーに基づいてセキュリティを確保した情報システムの構築・運営が行われている。このような動向は、官公庁から自治体、そして取引先である大手企業に広がる傾向にあり、大手企業の取引先である中小企業へとその動きが広がっていくことが容易に予想できる。この動向そのものは、健全な情報システムの構築を加速させるものとして歓迎すべきである。

【0004】

また、上記のような情報システムに設定するセキュリティポリシー（通常ポリシーファイルという形式で設定される）には、例えば、Java（登録商標）に設定するプログラムの実行許諾に関する設定情報や、ファイアウォールに設定す

るプロトコルの通過許可に関する設定情報などがある。

【0 0 0 5】

一般に、情報システムのセキュリティの確保は、機密性、完全性、可用性の確保に大別される。完全性や可用性は情報システムの管理者が適切に運営・管理すれば、実質上問題のないレベルを確保できる場合が多い。一方、機密性の確保のためには、中小企業に代表される情報システムのユーザー組織に所属するユーザーのそれぞれにセキュリティポリシーを共有・徹底させなければならない。このような理由で、特に、情報システムのコンテナである文書に対するポリシー、中でも機密保持に関するポリシーが重要視されているため、多くの企業では、文書に関するセキュリティを制御する要求が高まっている。

【0 0 0 6】

例えば、従来技術として、データファイルへのアクセスに対応するポリシーの評価を行う手段に加えて、ポリシーに条件が記述してあり、その条件をクリアにするための実行手段がある場合には、それを執行することでアクセス許可の評価を行っている（例えば、特許文献 1 参照）。しかしながら、データファイルへのアクセス制御システムであって、アクセス後のデータの処理、特に複写などには言及されていない。

【0 0 0 7】

また、従来技術として、ポリシー、システム、制御手段で構成され、それぞれの組み合わせが登録された DB から制御手段を抽出して、システムをポリシーに合うように制御する手段と、その状態を監査する手段とを有する（例えば、特許文献 2 参照）。しかしながら、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低いという問題がある。

【0 0 0 8】

また、従来技術として、ファイルへのアクセス制御をポリシーファイル（記述を列挙してある）に基づいて行い、単一システムによる制御及び制御部を分離したもの、複数の OS による制御、サーバクライアントプロセスによる制御などを行っている（例えば、特許文献 3 参照）。

【0 0 0 9】

また、従来技術として、第三者機関にセキュリティポリシーを設定、更新し、ネットワークを介してアクセス制御を行い、セキュリティ侵害の収集、解析、警告、否認不可保証を行い、異なるネットワークのオブジェクトを関連付けて、他のネットワークへのアクセスを管理し、関連付けられたオブジェクトの不整合を調整し、セキュリティポリシーに従って動作する機能のAPI (Application Program Interface) を提供する (例えば、特許文献4 参照)。

【0010】

また、従来技術として、ユーザーの証明書の確認を行うか否かをセキュリティポリシーに記述し、確認の方法には、唯一のユーザを特定できる高レベル、クライアントの認証結果を利用する中レベル、利用するプロトコルから判断する低レベルの3レベルがあり、低レベルで確認されたユーザは高いレベルで確認されたユーザのジョブに対してオペレーションできないなどのオペレーションの制御を行っている (例えば、特許文献5 参照)。

【0011】

また、従来技術として、セキュリティ管理者はユーザー、グループをサイト (プリンタ) のセキュリティレベルに応じてセキュリティ管理を行い、サイト (プリンタ) 管理者はプリンタのジョブの実行制限を行い、ユーザはパスワードなしで自分のファイルを表示印刷される場合に「禁止」などのラベルを付加できる (例えば、特許文献6 参照)。

【0012】

【特許文献1】

特開 2001-184264 号公報

【特許文献2】

特開 2001-273388 号公報

【特許文献3】

特開 2001-337864 号公報

【特許文献4】

特開平 7-141296 号公報

【特許文献 5】

特開平 9-293036 号公報

【特許文献 6】

特許第 2735966 号明細書。

【0013】

【発明が解決しようとする課題】

上記のように現在、多くの企業ではセキュリティポリシーを設け、そのセキュリティポリシーを制御しようとしているが、実際、オフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティポリシーではなく、オフィスシステムを構成するさまざまな情報システムに関して、個別にセキュリティ設定を行う必要がある。従って、このようなセキュリティ設定を行うためにさまざまな情報システムに関する知識が必要となってしまうという問題点があった。

【0014】

また、複数の情報システムの一つ一つにセキュリティポリシーを設定しなければならず、手間が煩雑になるという問題点があった。

【0015】

このように従来の複数の情報システムでは個別にセキュリティ設定を行っているため、情報システム全体がどのようなセキュリティ状態になっているかを把握するのが難しいという問題点があった。

【0016】

一方、従来の複数の情報システムのそれぞれにセキュリティの設定を行うことができても、実際に文書のセキュリティが守られていることをユーザーは明確に認識することができないという問題点があった。

【0017】

そこで、本発明の課題は、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる複写方法、記録媒体、伝送装置及び複写装置を提供することである。

【0018】

【課題を解決するための手段】

上記の課題を解決するため、本発明は、複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、複写する情報を読み取る読取手順と、上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有する構成とされる。

【0019】

このような複写方法では、複写する情報を読み取り、読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得し、文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断し、判断結果に基づいて、読取情報を所定の媒体に印刷させることにより、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【0020】

複写を指示するユーザーのセキュリティを判断するという観点から、本発明は、請求項2に記載されるように、更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手順を有し、上記判断手順は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手順により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断するように構成することができる。

【0021】

このような複写方法では、更に、複写を指示したユーザーに関する情報を取得し、判断手順は、文書のセキュリティが所定値以上のとき、取得されたユーザー情報と文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断することにより、複写を指示したユーザーによる複写が可能であるかを判断することができる。

【0022】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項3に記載されるように、上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むように構成することができる。

【0023】

このような複写方法では、セキュリティポリシーは、複写する読取情報に電子透かしを付加して印刷する要件を含むことにより、読取情報に電子透かしを入れて印刷するように複写処理を制御することができる。

【0024】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項4に記載されるように、上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むように構成することができる。

【0025】

このような複写方法では、セキュリティポリシーは、複写する読取情報にバーコードを付加して印刷する要件を含むことにより、読取情報にバーコードを入れて印刷するように複写処理を制御することができる。

【0026】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項5に記載されるように、上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むように構成することができる。

【0027】

このような複写方法では、セキュリティポリシーは、複写する読取情報を特定の媒体に印刷する要件を含むことにより、柔軟に文書のオペレーションを制御することができると共に、読取情報を特定の媒体に印刷するように複写処理を制御することができる。

【0028】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項6に記載されるように、上記セキュリティポリシーは、上記ユーザーにより複写が指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの

時刻とを履歴情報として格納する要件を含むように構成することができる。

【0029】

このような複写方法では、セキュリティポリシーは、ユーザーにより複写が指示されたとき、ユーザー情報と、読取情報と、複写を指示したときの時刻とを履歴情報として格納する要件を含むことにより、ユーザーは読取情報のセキュリティ状態や、複写処理の印刷状態を把握することができる。

【0030】

また、上記課題を解決するため、本発明は、上記複写方法における処理をコンピュータに実行させるプログラム、そのプログラムを格納した記録媒体、ネットワークを介して複写方法における処理を伝送するための伝送装置、及び複写装置とすることもできる。

【0031】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。本発明の実施の一形態に係る複写方法は、複写装置において、文書に関して生成されたセキュリティポリシーに基づいて複写処理を制御する。その複写装置のハードウェア構成は、例えば、図1に示すようになっている。

【0032】

図1は、本発明の実施の一形態に係る複写装置のハードウェア構成を示すブロック図である。

【0033】

図1において、複写装置10は、CPU11と、ROM12と、RAM13と、HDD14と、スキャナ15と、プロッタ16と、表示操作部17と、NIC (Network Interface Card) 18とで構成される。これらの各ユニットはバス19を介して接続されている。CPU11は、ROM12に格納された複写装置を制御するためのプログラム、及びHDD14からRAM13に転送されるプログラムとに基づいて、複写装置10を制御する。また、CPU11は、RAM13を作業メモリ空間として利用すると共に、RAM13から処理対象のデータを読み出して処理する。処理後のデータはRAM13に格納

される。HDD 14 は、文書ファイル、複写方法に係るプログラムなどを格納する。スキャナ 15 は、印刷物をスキャンして電子データとして取り込むスキャナ処理を行う。プロッタ 16 は、パーソナルコンピュータ（PC）などで生成した電子文書を印刷する場合や、印刷物などを複写する印刷処理を行う。NIC 18 は、ネットワークインターフェースであり、ネットワークと接続されて複数の情報システムとセキュリティポリシーなどの複写方法に関する情報の送受信を行う。表示操作部 17 は、オペレーションパネルなどで構成され、ユーザからの入力操作の受け付け並びにユーザに向けた表示を行う。

【0034】

このようなハードウェア構成を採用することにより、複数の情報システム、特に複写装置 10 のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【0035】

尚、セキュリティポリシー 100 を記録する記録媒体は、上記 ROM 12、RAM 13、HDD 14 に限定されることなく、セキュリティポリシー 100 を記録することができ、コンピュータが読み取り可能な媒体であれば適応可能である。

【0036】

図 2 は、本発明の実施の一形態に係る複写方法におけるシステム構成図である。図 2 において、複写方法に係る複写装置 10 は、ネットワーク 1 を介して、他の複写装置、ファックス、プリンタなどの複数の情報システム 30 に接続される。複写装置 10 は、文書に関するセキュリティポリシー 100 と、ユーザーによる複写指示の入力操作並びに複写処理に関する通知が行われるオペレーションパネル 21 と、複写する印刷物などから情報を読み取る読み取り処理部 22 と、複写を行うユーザーの属性を取得するユーザー属性取得処理部 23 と、複写する文書に関する属性を取得する文書属性取得処理部 24 と、セキュリティポリシー 100 に基づいて印刷処理を行う印刷処理部 25 と、読み取り処理部 22 により読み取られた情報を格納する読み取り情報 DB 26 と、文書の属性情報が格納された文書属性 DB 27 と、ユーザーの属性情報が格納されたユーザー属性 DB 28

とで構成される。この複写装置 10 は、図 1 に示す CPU 11（中央処理装置）によって各構成が制御される。

【0037】

以下に、複写装置 10 で行われる複写処理の手順について説明する。

ユーザーにより、複写装置 10 のオペレーションパネル 21 から複写指示が入力されると、オペレーションパネル 21 は、読み取り処理部 22、ユーザー属性取得処理部 23 に複写指示を供給する。読み取り処理部 22 は、複写指示に応じて印刷物から複写する情報を読み取り、読み取り情報 DB 26 に格納する。また、読み取り処理部 22 は、文書属性取得処理部 24 に読み取り情報を供給する。文書属性取得処理部 24 は、読み取り情報に基づいて、文書属性 DB 27 に格納された文書属性を取得し、取得した文書属性を読み取り処理部 22 及び印刷処理部 25 に供給する。読み取り処理部 22 及び印刷処理部 25 は、文書属性とセキュリティポリシー 100 とに基づいて、セキュリティポリシー 100 に記述された文書の要件を満たしているかを判断する。

【0038】

更に、読み取り処理部 22 及び印刷処理部 25 は、判断結果から必要に応じて、ユーザー属性処理部 23 にユーザー属性の要求を供給する。ユーザー属性処理部 23 は、オペレーションパネル 21 にユーザー情報の入力を促す情報の表示を指示し、ユーザー情報を取得する。ユーザー属性処理部 23 は、ユーザー情報に基づいて、ユーザー属性 DB 28 に格納されたユーザー属性を読み取り処理部 22 及び印刷処理部 25 に供給する。読み取り処理部 22 及び印刷処理部 25 は、ユーザー属性処理部 23 からのユーザー属性に基づいて、セキュリティポリシー 100 に記述されたユーザーの要件を満たしているかを判断する。印刷処理部 25 は、判断結果に応じて読み取り情報を印刷する。読み取り処理部 22 は、印刷結果をオペレーションパネル 21 に表示する指示を供給する。

【0039】

尚、複写装置 10 は、上記一連の複写処理を実行するためのプログラムを、ネットワーク 1 を介して情報システム 30 に伝送することで、複数の情報システム 30、特に、他の複写装置のセキュリティポリシーを共有させることができる。

従って、複数の情報システムのセキュリティポリシーを統括して管理することが可能となる。

【0040】

次に、文書に関するセキュリティポリシー100の記述について説明する。尚、セキュリティポリシー100は、XML (eXtensible Markup Language) 形式で記述するものとする。図3は、文書に関するセキュリティポリシーの例を示す図である。図3において、セキュリティポリシー100には、記述120と記述121に示す<policy>と</policy>とで囲まれた範囲の記述101～110、122、123に、文書に関するセキュリティポリシーの要件が設定されている。記述120には、セキュリティポリシー100を識別するための情報が記述されている。記述122、123に示す<ace_rule>は、文書に対して許可される操作（オペレーション）や、ユーザーに対するオペレーションの許可に関する要件が設定されている。

【0041】

まず、記述122の要件について説明する。

【0042】

記述101示す文書のカテゴリ<doc_category>には、どの文書のカテゴリにも適応する「ANY」が設定されている。記述102に示す文書のセキュリティレベル<doc_security_level>には、文書のセキュリティレベルが標準であることを示す「basic」が設定されている。記述103に示すユーザーのカテゴリ<user_category>には、どのユーザーのカテゴリにも適応する「ANY」が設定されている。記述104に示すユーザーのセキュリティレベル<user_security_level>には、どのユーザーにも適応する「ANY」が設定されている。記述105に示す<name>hardcopy</name><allowed/>は、複写処理を要件なく許可することを示している。

【0043】

次に、記述123の要件について説明する。

【0044】

記述106示す文書のカテゴリ<doc_category>には、どの文書のカテゴリに

も適応する「ANY」が設定されている。記述107に示す文書のセキュリティレベル<doc_security_level>には、文書のセキュリティレベルの高いことを示す「high」が設定されている。記述108に示すユーザーのカテゴリ<user_category>には、ユーザーのカテゴリと文書のカテゴリが同等であることを示す「DOC-CATEGORY」が設定されている。記述109に示すユーザーのセキュリティレベル<user_security_level>には、どのユーザーにも適応する「ANY」が設定されている。記述110に示す<name>hardcopy</name><requirement>audit</requirement><requirement>embed_trace_info</requirement>は、複写処理において、印刷履歴情報を記録する要件と、追跡可能な情報を埋め込む要件を満たすときに許可することを示している。

【0045】

このように、複写装置10は、要件が設定されたセキュリティポリシー100に基づいて複写処理を行うことにより、文書及びユーザーのセキュリティの要件を満たした複写処理を行うことができる。また、セキュリティポリシー100がXML形式で記述されていることにより、プラットフォームに依存せずに情報システム30全体にセキュリティポリシーを共有させることができる。

【0046】

尚、上記印刷履歴情報を記録する要件において、ユーザーによりオペレーションパネル21から複写が指示されたときにユーザー情報、読取情報、複写を指示したときの時刻などを記録するように設定してもよい。

【0047】

次に、上記複写装置10で実行される複写処理の手順について説明する。図4は、複写処理を説明するためのフローチャート図である。図4において、まず、ステップS10の処理で、ユーザーにより複写装置10に紙文書が読み取り処理部22にセットされた状態で、オペレーションパネル21に複写指示が入力されると、オペレーションパネル21から読み取り処理部22及びユーザー属性取得処理部23に複写指示が供給される。ステップS11の処理で、読み取り処理部22は、紙文書から複写する情報を読み取り、読み取り情報DB26に読み取り情報を格納すると共に、印刷処理部25及び文書属性取得処理部24に読み取り

情報を供給する。ステップS12の処理で、文書属性取得処理部24は、読み取り情報に基づいて、文書属性DB27に格納された文書属性を取得し、読み取り処理部22及び印刷処理部25に供給する。尚、文書属性取得処理部24は、読み取り情報のバーコードや、電子透かし等の画像情報から文書のIDを抽出して、文書属性DB27に格納された文書属性を取得するようにしてもよい。

【0048】

ステップS13の処理で、読み取り処理部22及び印刷処理部25は、セキュリティポリシー100及び文書属性とに基づいて、その文書の複写に対する要件が有るか否かを判断する。例えば、ステップS12の処理において、複写する文書情報のセキュリティレベルが、図2に示すセキュリティポリシー100に設定されている、文書のセキュリティレベル「basic」の場合、要件がないものと判断される。また、複写する文書情報のセキュリティレベルが、文書のセキュリティレベル「high」の場合、印刷履歴情報を記録する要件と、追跡可能な情報を埋め込む要件があるものと判断される。

【0049】

ステップS13の処理で、その文書の複写に対する要件が有る場合、ステップS14の処理で、読み取り処理部22及び印刷処理部25は、その要件全てを満たすか否かを判断する。ステップS14の処理で、その要件全てを満たさない場合、ステップS16の処理で、読み取り処理部22及び印刷処理部25は、読み取った文書情報を破棄して印刷を中止すると共に、ユーザーに通知するためにオペレーションパネル21に印刷中止の情報を供給する。ステップS14の処理で、その要件全てを満たす場合、ステップS17の処理で、読み取り処理部22及び印刷処理部25は、読み取った文書情報を印刷する。例えば、ステップS17の処理は、複写する文書情報のセキュリティレベルが、図2に示すセキュリティポリシー100に設定されている、文書のセキュリティレベル「high」の場合に実行される。具体的には、第1に、ユーザー属性取得処理部23は、オペレーションパネル21から複写指示を出したユーザーにユーザーIDの入力を促す情報の表示を指示する。第2に、ユーザーは、オペレーションパネル21からユーザーIDを入力する。第3に、ユーザー属性取得処理部23は、ユーザーIDに基

づいて、ユーザー属性DB 28に格納されているユーザー属性から入力されたユーザーIDに対応するカテゴリ、セキュリティレベルを取得し、読み取り処理部22と印刷処理部25とに供給する。第4に、読み取り処理部22又は印刷処理部25のどちらか一方が、印刷履歴情報を記録する。第5に、印刷処理部25は、追跡可能な情報の埋め込み、例えば、電子透かし、バーコードなどを追加して印刷を行い、複写処理を終了する。

【0050】

一方、ステップS13の処理で、その文書の複写に対する要件がない場合、ステップS15の処理で、印刷処理部25は、読み取った文書情報を印刷し、複写処理を終了する。例えば、ステップS13の処理は、複写する文書情報のセキュリティレベルが、図2に示すセキュリティポリシー100に設定されている、文書のセキュリティレベル「basic」の場合に実行される。

【0051】

このように、上記複写方法において、ユーザーによりオペレーションパネル21から複写指示があると、読取処理部22により複写する情報を読み取り、文書属性取得処理部24により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性を取得し、読取処理部22、印刷処理部25により文書属性とセキュリティポリシー100とに基づいて、読取情報が複写可能であるか否かを判断して読取情報を印刷することにより、そのセキュリティポリシー100を反映させた複写処理を行うことができる。更に、ユーザー属性取得処理部23により複写を指示したユーザーに関する情報を取得し、読取処理部22、印刷処理部25によりユーザー属性情報と文書属性とセキュリティポリシー100とに基づいて、読取情報が複写可能であるか否かを判断することにより、複写を指示したユーザーによる複写が可能であるかを判断することができる。

【0052】

また、上記複写方法における処理を、複数の情報システムに伝送することにより、特に複数の複写装置に共通のセキュリティポリシー100を統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる

尚、上記複写処理において読み取られた紙文書の情報を複写する媒体は、紙に

限定されることなく、OCR用の特定の印刷用紙などにも適応可能である。

【0053】

【発明の効果】

上述の如く本発明によれば、複写する情報を読み取り、読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得し、文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断し、判断結果に基づいて、読取情報を所定の媒体に印刷させることにより、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【図面の簡単な説明】

【図1】

本発明の実施の一形態に係る複写装置のハードウェア構成を示すブロック図である。

【図2】

本発明の実施の一形態に係る複写方法におけるシステム構成図である。

【図3】

文書に関するセキュリティポリシーの例を示す図である。

【図4】

複写処理を説明するためのフローチャート図である。

【符号の説明】

1	ネットワーク
10	複写装置
11	CPU
12	ROM
13	RAM
14	HDD
15	スキャナ
16	プロッタ
17	表示操作部

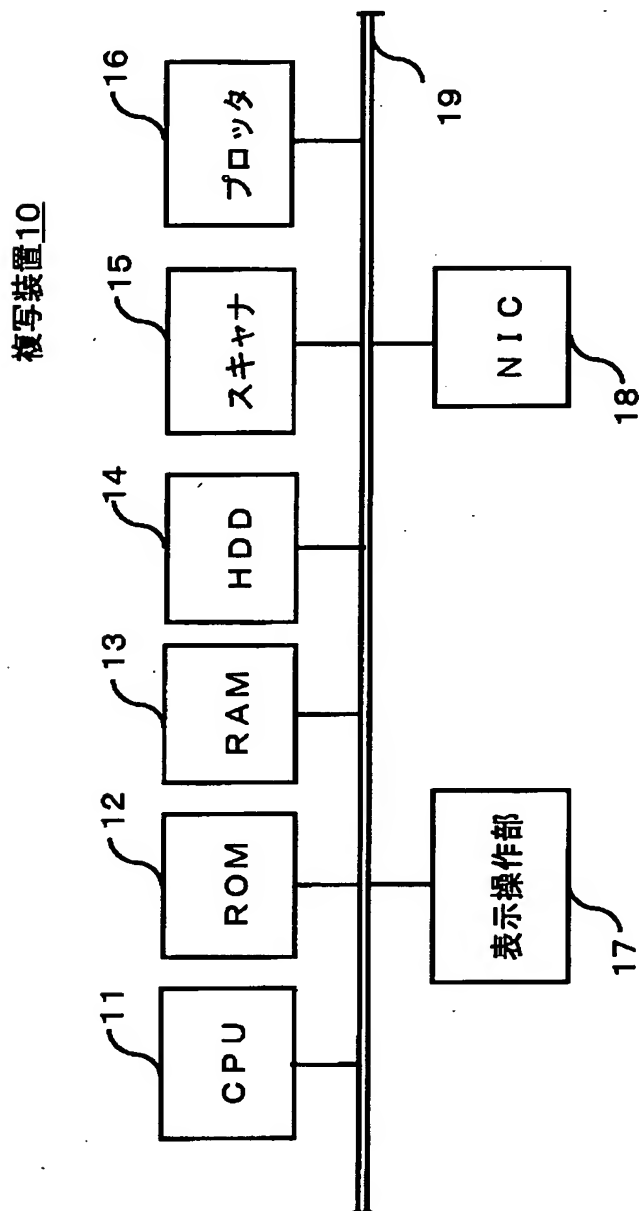
1 8	N I C
1 9	バス
2 1	オペレーションパネル
2 2	読み取り処理部
2 3	ユーザー属性取得処理部
2 4	文書属性取得処理部
2 5	印刷処理部
2 6	読み取り情報 D B
2 7	文書属性 D B
2 8	ユーザー属性 D B
3 0	情報システム
1 0 0	セキュリティポリシー

【書類名】

図面

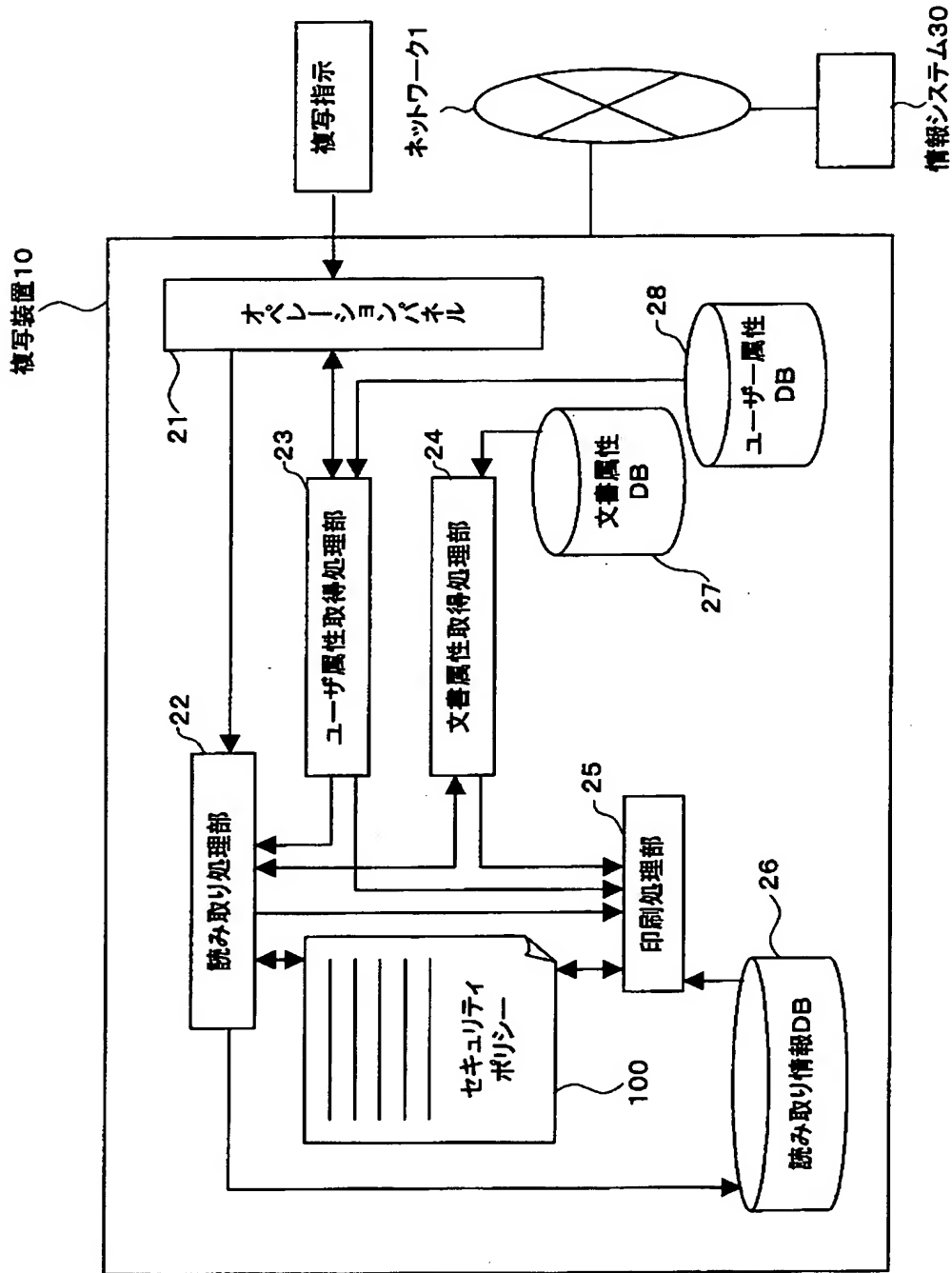
【図 1】

本発明の実施の一形態に係る複写装置の
ハードウェア構成を示すブロック図



【図 2】

本発明の実施の一形態に係る複写方法における
システム構成図



【図 3】

文書に関するセキュリティポリシーの例を示す図

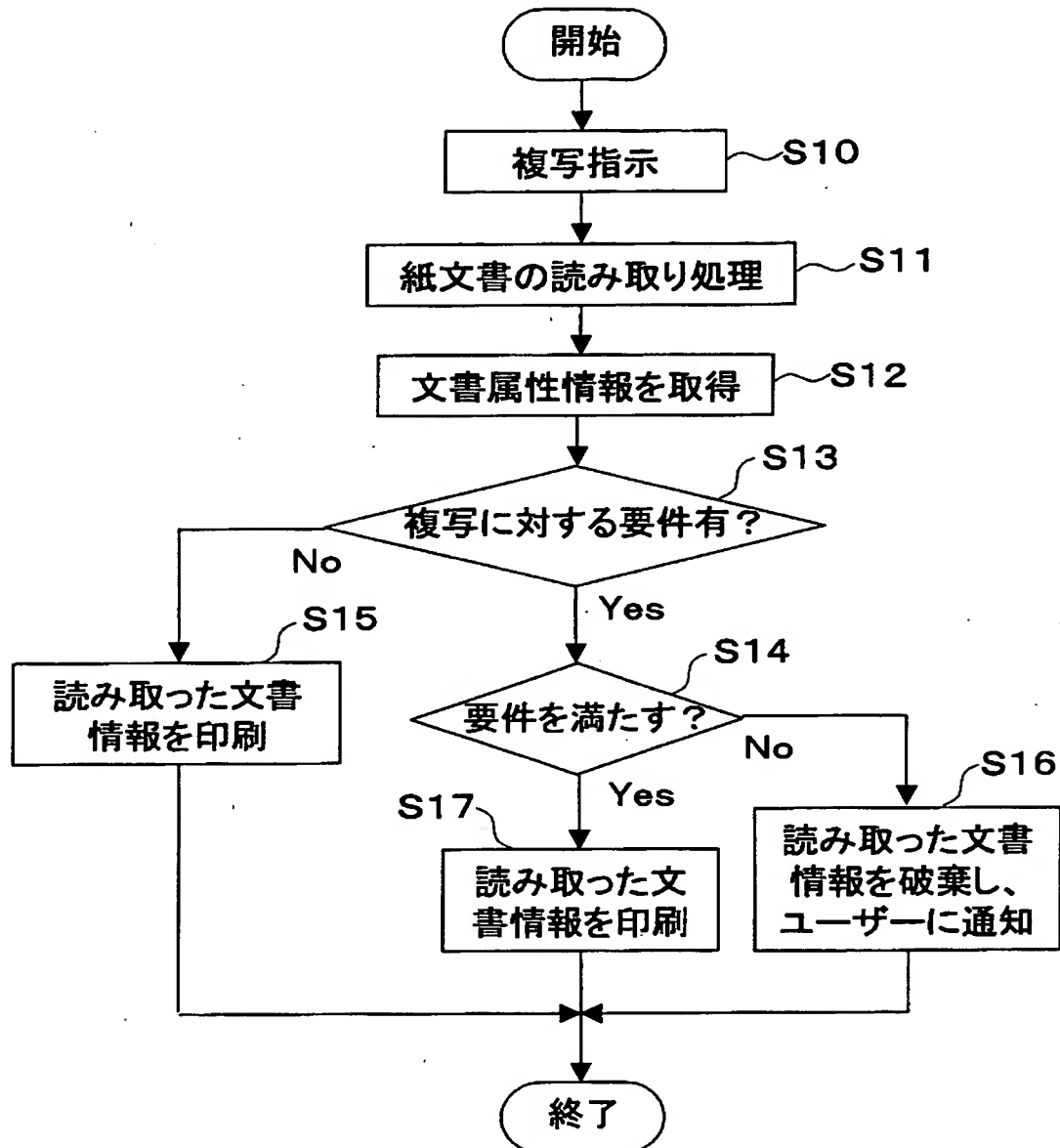
```

100 {
120  <?xml version="1.0" encoding="SHIFT-JIS" ?>
121  <document_security_policy>
122  <policy>
123  <acc_rule>
101  <doc_category>ANY</doc_category>
102  <doc_security_level>basic</doc_security_level>
103  <ace>
104  <user_category>ANY</user_category>
105  <user_security_level>ANY</user_security_level>
106  <operation>
107  <name>hardcopy</name>
108  <allowed/><!--allowed without any requirement-->
109  </operation>
110  </ace>
111  </acc_rule>
112  </policy>
113  </document_security_policy>
114  </xml>

```

【図 4】

複写処理を説明するためのフローチャート図



【書類名】 要約書

【要約】

【課題】 複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる複写方法を提供することを目的とする。

【解決手段】 本発明の課題は、複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、複写する情報を読み取る読取手順と、上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有する構成とされる。

【選択図】 図2

特願 2002-273985

出 願 人 履 歴 情 報

識別番号

[000006747]

1. 変更年月日 1990年 8月24日
 [変更理由] 新規登録
 住 所 東京都大田区中馬込1丁目3番6号
 氏 名 株式会社リコー

2. 変更年月日 2002年 5月17日
 [変更理由] 住所変更
 住 所 東京都大田区中馬込1丁目3番6号
 氏 名 株式会社リコー